DECLARATION OF MARK W. PERLIN

United States of America v. Lafon Ellis

I, Mark W. Perlin, declare I have personal knowledge of the following, and if called upon to do so, could and would testify competently to the matters contained herein:

1. I hold the following academic degrees: a B.A. in Chemistry from SUNY/Binghamton, a Ph.D. in Mathematics from CUNY/Graduate School, an M.D. from the University of Chicago Pritzker School of Medicine, and a Ph.D. in Computer Science from Carnegie Mellon University. I have been issued thirteen patents. Prior to founding my own technology company, I was a senior research faculty member of Carnegie Mellon University's School of Computer Science. I have been qualified to testify as an expert in thirty-five jurisdictions. I am currently a scholar-in-residence faculty member in the Forensic Science and Law program at Duquesne University.
2. Cybergenetics is a Pennsylvania corporation located at 160 North Craig Street, Suite 210, Pittsburgh, PA 15213. Cybergenetics is the owner of the TrueAllele® software, as well as its proprietary source code.

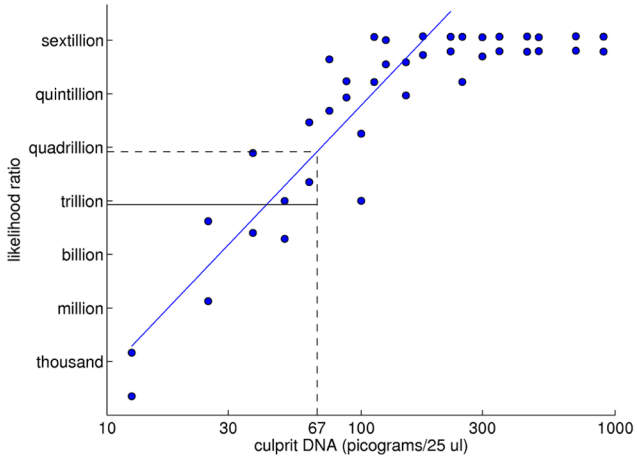
The DNA is the evidence

3. When someone leaves unexplained DNA on an item used in a crime, that DNA associating them with the crime becomes potentially probative evidence. Forensic scientists can transform DNA molecules sampled from the item into DNA data.
4. The DNA identification hypothesis (H) is that a suspect left his DNA on the item. The alternative hypothesis ($\overline{\mathrm{H}}$) is that the DNA was left by someone else.

5. Scientifically weighing the evidence gives the statistical weight (W) for hypothesis H in the data. This weight is determined by comparing how well H explains the data, relative to how well $\overline{H}$ explains the data.
6. Mathematically, this weight is expressed as the base ten logarithm of the ratio of the probability of the data under each of the two different hypotheses. That ratio of data probabilities is called the likelihood ratio (LR). *See: Good IJ. Probability and the Weighing of Evidence. London: Griffin; 1950.*
7. When this LR logarithm is a large number (much greater than 1), the evidence supports the hypothesis. When the log(LR) is small (much lower than 1), the evidence does not support the hypothesis. When the log(LR) is around zero, there is no support in the data either way.

Weighing the DNA evidence

8. The weight of evidence W is a true, quantifiable number of the evidence data, relative to the hypothesis H. The weight W expresses the amount of identification information that the evidence data contain for the hypothesis.
9. With low-level DNA mixtures, there is a straight-line log-log relationship between the amount of DNA a contributor leaves in a mixture (x-axis) and the amount of identification information (y-axis). This predictive linear relationship between DNA quantity and information has been confirmed in published peer-reviewed scientific studies, as shown in the figure below (*PLoS ONE, 2009*; Figure 9). *See: Perlin MW, Sinelnikov A. An information gap in DNA evidence interpretation. PLoS ONE. 2009;4(12):e8327*; *Perlin MW, Hornyak J, Sugimoto G, Miller K. TrueAllele® genotype identification on DNA mixtures containing up to five unknown contributors. J Forensic Sci. 2015;60(4):857-68.*



Using a linear relationship to predict match information from DNA quantity in Pennsylvania v. Foley.

10. The data's DNA identification information can be weighed through statistical modeling. Better methods that make full use of the data can find the full weight of evidence. Limited methods that make less use of the data may underestimate evidential weight.

11. The weight of evidence is an inherent property of the biological DNA evidence. This evidence is observed through the laboratory's DNA data. When using better methods to model DNA data, different computer programs will measure the same statistical weight.

Testing software reliability

12. Scientists test the reliability of their measuring scales. For measuring the weight of DNA evidence, this is done through validation studies that test statistical software methods on actual DNA data. The testing determines error rates. For a developmental validation, the manufacturer's study results are published in a peer-reviewed scientific journal.

13. Courts require scientific methodologies to be tested for their reliability. *See: Daubert v. Merrell Dow Pharmaceuticals Inc., 509 U.S. 579 (1993)*. Under the *Daubert* standard, the factors that may be considered in determining whether the methodology is valid

are: (1) whether the theory or technique in question can be and has been tested; (2) whether it has been subjected to peer review and publication; (3) its known or potential error rate; (4) the existence and maintenance of standards controlling its operation; and (5) whether it has attracted widespread acceptance within a relevant scientific community. With the weight of DNA evidence, the nationally accepted standard for methodological testing is applying software to DNA mixture data and assessing the resulting weights.

14. Nonscientists opposing DNA software methods generally do not test the software. They do not adhere to the Daubert standard, national DNA software testing standards, or any other widely accepted scientific testing standard. Rather, they propose to dismantle the software, taking apart the weighing scale instead of testing its reliability. To dismantle the software, they request its source code.

Algorithms, source code, and executable software

15. Software development has three phases. First, designers specify *algorithm* methods that can solve a problem. Second, programmers translate the algorithms into *source code* text that a computer can read. Third, a computer transforms the source code into an *executable* software application that can be run on input data.

16. Cybergenetics publishes its TrueAllele *algorithms* in scientific journals, patent specifications, and other documents that are publicly available. The company makes the *executable* TrueAllele software application available to defendants free of charge for their scientific testing.

17. TrueAllele source code is a protected trade secret. TrueAllele publications, not the source code, enable a qualified expert to understand the disclosed algorithms. The available executable software, not source code, is used to test the application software on DNA data.

18. Trade secrets enable innovation. Proprietary source code is not needed for testing software reliability, under legal or scientific standards. But disclosing source code can eviscerate technological innovation. Revealing trade secrets to competitors eliminates incentives to invest time and resources into innovating new products, and can ruin a company.

19. Such commercial progress innovated the reliable weighing of DNA evidence, bringing accurate and objective scientific evidence into the courtroom. Unlike previous limited methods, these innovative scientific scales correctly weigh the DNA evidence, and give impartial readings that can favor either side.

The DNA evidence in this case

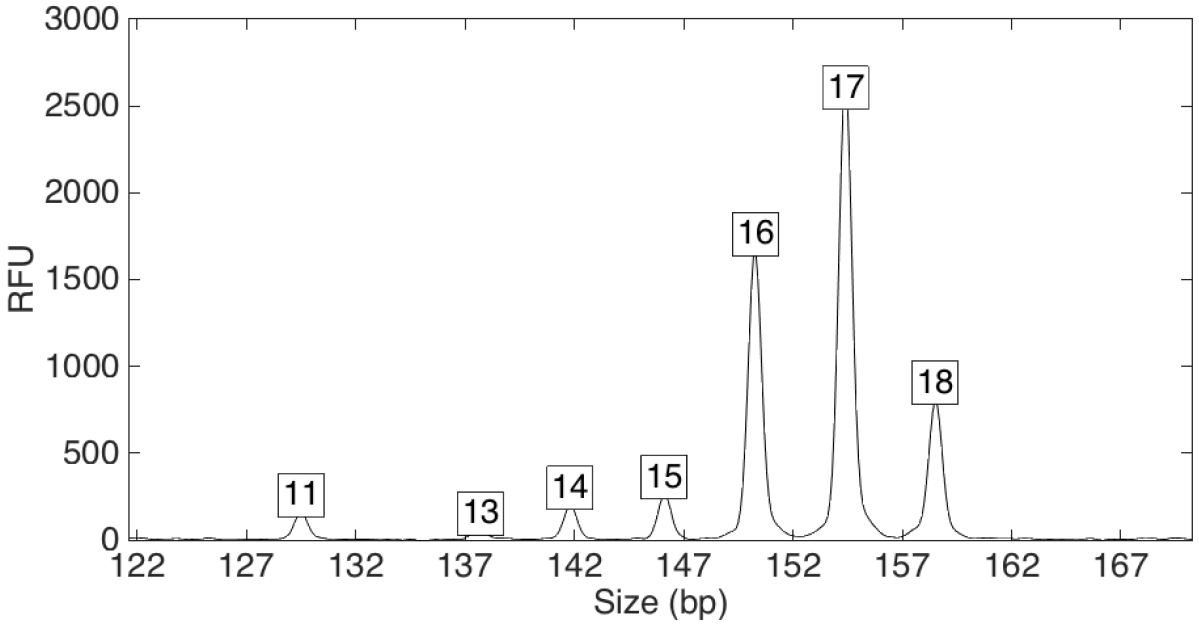
20. The DNA evidence in this case was the swabbing of pistol (Item 2A, Sig Sauer SP2022 40 Pistol).

21. The Allegheny County Medical Examiner's (ACME) Office crime laboratory isolated DNA from the pistol. Using polymerase chain reaction (PCR), the lab amplified the DNA using a Power Plex® Fusion 6C short tandem repeat (STR) kit to produce DNA electropherogram (EPG) data at 23 STR loci.

22. The ACME uses limited human review DNA interpretation methods that are generally unable to produce a reliable result from complex mixtures. In this case, the ACME lab did not report any identification information from their EPG data. *See: Perlin MW. Inclusion*

probability for DNA mixtures is a subjective one-sided match statistic unrelated to identification information. J Pathol Inform. 2015;6(1):59.

23. The DNA mixture EPG data from the pistol at locus vWA is shown in the figure below. The horizontal x-axis shows DNA fragment length in base pair (bp) units, while the vertical y-axis shows the relative fluorescence unit (RFU) peak heights detected at each allele. The allele values are indicated by a boxed number atop each labeled peak.



24. The genotype of Lafon Ellis at the vWA locus is a (16, 17) allele pair. At this locus, his DNA appears to be present in the pistol DNA mixture, corresponding to the two tallest peaks.

25. To use DNA evidence in a court of law, a match statistic is needed to describe the weight of evidence between the evidence and a suspect. The weight numerically indicates to what extent the suspect's DNA is present or absent from the DNA evidence.

Software for measuring DNA identification information

26. To weigh DNA evidence, different probabilistic genotyping software programs can examine identical DNA data. Concordance between the different weights of evidence would show that the evidential weight W resides in the evidence, not in a particular software program.

27. DNA evidence is weighed by calculating a likelihood ratio. The LR expresses the odds of the identification hypothesis H after examining DNA data, relative to the odds without the data. The "likelihood" of a hypothesis is the probability of obtaining the observed data when assuming that hypothesis. The LR can be written as a ratio of likelihoods.

28. The LR is numerically calculated from genotype probabilities derived from the DNA data. The *probability* of a genotype allele pair value is the product of its *likelihood* (how well the genotype explains the EPG data) times its *prevalence* (how frequently the genotype appears in a human population). In some formulations, only genotype likelihood is used.

29. PCR amplification is an imperfect copying mechanism that introduces a random element into the DNA data. At each of the 28 PCR cycles, with some probability, an allele may be copied or not. Thus, different PCR experiments on the same DNA material produce different EPG allele patterns.

30. Probabilistic genotyping (PG) methods can account for this PCR data variation. PG software can also handle other PCR artifacts of low-level DNA mixtures, such as PCR stutter or heterozygote imbalance.

31. Human review weight of evidence methods treat data in an all-or-none way, applying RFU thresholds that discard EPG data. They only consider the presence or absence of alleles, and ignore their peak heights. These mixture interpretation methods lose considerable

identification information, and often report no result. Formally, they are a PG method where the likelihood value is either zero or one.

32. "Drop out" (or "semi-continuous") weight of evidence methods remedy threshold data loss by introducing a numerical drop out factor that accounts for the loss of detectable alleles during PCR amplification. They do apply thresholds, considering only the presence or absence of allele data. But the drop out factor ensures that the likelihood of an allele never reaches zero, so that all genotype possibilities can be considered.

33. Three well-known drop out software programs are LRmix, Lab Retriever, and likeLTD version 5. These PG applications are freely available for download from the Internet. Moreover, they are open source, meaning that their computer source code can be downloaded as well.

34. "Data modeling" (or "continuous") weight of evidence methods use EPG peak heights. These PG methods explain (rather than discard) DNA mixture data by adding together possible contributor genotypes to form a proposed EPG pattern. The more likely genotype combinations better explain the EPG data. These methods measure PCR allele variation from the data, using the variation to help compute genotype probability.

35. Three well-known data modeling software programs are likeLTD version 6, EuroForMix, and TrueAllele. The first two PG applications are freely available for download from the Internet. They are open source, so their computer source code can be downloaded as well.

36. All six of these PG programs were run on the pistol DNA mixture data in this case. The table below shows the software settings. *See Cybergenetics supplemental report, dated October 23, 2020, page 2.* The programs used prosecution hypothesis H_p and defense hypothesis H_d to calculate the LR weight of evidence.

	Drop out software			Data modeling software		
Input settings	LRmix	Lab Retriever	likeLTD, v 5.5	likeLTD, v 6.3	EuroForMix	TrueAllele
Data threshold	50 rfu	50 rfu	50 rfu	20 rfu	50 rfu	
Stutter modeled	No	No	No	Yes	Yes	Yes
Total loci used	22	21	16	16	21	23
Loci omitted	SE33	Penta D, Penta E	CSF1PO, D5S818, D7S820, D13S317, Penta D, Penta E, TPOX	D2S1338, D12S391, D18S51, D22S1045, Penta D, Penta E, SE33	Penta D, Penta E	
Pr(Dropin)	0.05	0.01	TRUE	TRUE	0.05	
Pr(Dropout)	0.1	0				
Degradation					Yes	Yes
H_p	suspect + 3 unknown	suspect + 3 unknown	suspect + 2 unknown + drop in	suspect + 2 unknown + drop in	suspect + 3 unknown	suspect + 3 unknown
H_d	4 unknown	4 unknown	3 unknown + drop in	3 unknown + drop in	4 unknown	4 unknown

Results from applying different PG software programs

37. Each of the six PG software programs calculated log(LR) weight of evidence values, comparing the genotypes of the pistol evidence (Item 2A) and Lafon Ellis (Reference 4). The LR and log(LR) values are shown in the table below. *See Cybergenetics supplemental report, dated October 23, 2020, page 3.*

	Drop out software			Data modeling software		
	LRmix	Lab Retriever	likeLTD, v 5.5	likeLTD, v 6.3	EuroForMix	TrueAllele
LR	1.44 thousand	110 thousand	36.7 thousand	721 million	2.02 quadrillion	21.4 trillion
log(LR)	3.16	5.04	4.57	8.86	15.31	13.33

38. The PG drop out programs gave concordant inclusionary results for the drop out method, with weights of evidence ranging from 3 to 5 ban units. ($\log_{10}$(LR) is measured in *ban* units.)

39. The PG data modeling programs gave concordant inclusionary results for the data modeling method, with weights of evidence ranging from 8 to 15 ban units. The likeLTD weight of

8.86 was lower because (a) it considered only 16 of 23 loci, and (b) the program can handle at most three unknown contributors. The EuroForMix weight of 15.31 was higher because it used a threshold of 50 RFU, which ignores potentially exculpatory allele data. The TrueAllele weight of 13.33 was the middle value.

40. Six different PG software programs weighed the same DNA data. Within each method, the programs found concordant weights of evidence W. All of the programs gave inclusionary weights from the DNA evidence that showed statistical support for Lafon Ellis having left his DNA on the pistol.

41. Using six different PG software programs, empirical testing of executable software on the DNA evidence reached the same conclusion. The more advanced data modeling methods found similar weights of evidence W. Specifically, EuroForMix found a weight of 15.31 ban, and TrueAllele a weight of 13.33 ban. This scientific result shows that the weight of evidence is a property of the DNA mixture evidence, not of the particular software used.

42. All six programs are available to the defense as executable software for their own independent testing. The defense can scientifically test these programs on the ACME pistol data to confirm our inclusionary findings.

43. It is highly unlikely that all six programs suffer from random coding defects that coincidently give the same inclusionary result, namely that the DNA evidence supports Lafon Ellis having left his DNA on the pistol. But five of the six programs have freely available source code that are not trade secrets. The defense can readily inspect the source code of these five programs to make their own determination.

TrueAllele reliability under the Daubert standard

44. TrueAllele has been found to be reliable in twenty-seven admissibility rulings in American courts, including in federal court. The admissibility criteria largely followed the Daubert prongs, particularly regarding empirical testing of the system.

45. TrueAllele software is testable, and it has been extensively tested in thirty-nine validation studies. The defense can test TrueAllele at no charge, should they wish to challenge the software's reliability based on empirical science.

46. TrueAllele's error rate has been documented in validation studies. The software includes tools for computing error rates, both for validation studies and LR match statistics. Cybergenetics reported an error rate for the LR in this case, stating: "For a match strength of 21.4 trillion, only 1 in 3.95 quadrillion people would match as strongly."

47. TrueAllele has been extensively peer-reviewed. In addition to methodological papers, there are eight peer-reviewed validation studies published in scientific journals.

48. TrueAllele has been empirically validated in accordance with national standards for validating probabilistic genotyping systems and other performance criteria. Cybergenetics has documented its compliance with these widely accepted forensic science testing standards. Specifically, these standards have been developed by (1) the Federal Bureau of Investigation (FBI) as Quality Assurance Standards (QAS) (see the "FBI QAS 2020" validation standard), (2) the FBI's Scientific Working Group for DNA Analysis Methods (see the "SWGDAM 2015" PG validation guidelines), and (3) the American National Standards Institute (ANSI) and American Academy of Forensic Sciences (AAFS) Standards Board (ASB)

in their ANSI/ASB Standards (see the "018-2020", "020-2018" and "040-2019" DNA mixture validation and interpretation standards).

49. TrueAllele enjoys widespread acceptance. Cybergenetics has issued over 900 reports in 44 states and federally. Ten crime laboratories use the software to interpret DNA mixtures. The results are used by prosecutors and defenders, and by police and innocence groups.

50. TrueAllele is accurate. Its match statistics are sensitive, specific and reproducible. Peer-reviewed validation studies have demonstrated the system's accuracy. *See: Perlin MW, Dormer K, Hornyak J, Schiermeier-Wood L, Greenspoon S. TrueAllele® Casework on Virginia DNA mixture evidence: computer and manual interpretation in 72 reported criminal cases. PLoS ONE. 2014;9(3):e92837.*

Transparency of TrueAllele methods and software

51. Cybergenetics has described its TrueAllele methods in scientific journals, patent specifications, disclosure documents, public talks, educational videos, book chapters, and user training for over twenty years. TrueAllele is an open book, not a black box.

52. Cybergenetics provides opposition attorneys with DNA laboratory data from the case, along with its own validation testing data.

53. Cybergenetics includes VUIer™ software for reviewing DNA data and TrueAllele results in its disclosure materials.

54. Cybergenetics invites opposition attorneys to test TrueAllele for free, providing access to the executable software application via the Internet. Scientific experts know how to test software on data, and review the results.

55. In software engineering, "validation" means determining and documenting whether software actually does what it was designed to do. In this sense, TrueAllele has been validated. Before using the software in casework, Cybergenetics thoroughly tests it at each development phase. The testing ensures that released software behaves according to its documented features. Moreover, over 35 validation studies, 8 published in peer-reviewed journals, document TrueAllele aspects. Each study shows that the software performs as intended and as expected.

56. In software engineering, "verification" means demonstrating and documenting that the software conforms to requirements and standards. In this sense, TrueAllele has been verified. Each step of software development has verification checks in which software, code, user interfaces, and installers are evaluated to ensure their accuracy and intended operation. Additionally, Cybergenetics checks and documents testing plans and software operation manuals. This ensures that the software conforms to its feature requirements.

57. Cybergenetics makes its TrueAllele source code available to defense teams under confidentiality agreements or protective orders that respect trade secrets.

TrueAllele source code

58. TrueAllele source code is a protected trade secret.

59. Computer source code is not useful for empirical testing of the software on forensic DNA data, nor for determining its error rate. Actual testing of an executable application on data can find coding errors, but source code inspection does not. *See: Taylor DA, Bright J-A, Buckleton J. Commentary: "Source" of Error: Computer Code, Criminal Defendants, and the Constitution. Front Genet. 2017;8:33; Buckleton JS, Curran J, Taylor D, Bright J-A. What can*

forensic probabilistic genotyping software developers learn from significant non-forensic software failures? WIREs Forensic Sci. 2020(e1398):1-8.

60. In September of this year, Cybergenetics made its source code available for defense inspection at its lawyer's office in a criminal case in Fairfax, Virginia, *Commonwealth v. Clark Watson*. The defense expert, Nathaniel Adams (who is also a defense expert in this case), never came to see it. Our Virginia lawyer, Brandon Shapiro, offered to drive out to Mr. Adams location with the source code; the defense declined the offer. Once the defenders were granted access to the source code, they no longer needed to see it or continue litigating the nonissue.

61. The court in *Comm. v. Watson* was alerted to TrueAllele's trade secret status. An appropriate protective order was issued on December 17th, 2020. The order does not provide unfettered access to trade secrets. Rather, the judge's order clearly states that:

62. "Cybergenetics shall make their source code available to counsel for the defendant, and any experts the defense may retain to review the source code for the TrueAllele software. Persons authorized to view the documents provided under this order may view the materials only at the office of Brandon Shapiro, Counsel for Cybergenetics, located at Carroll & Nuttall, P.C., 10521 Judicial Drive, Suite 110, Fairfax, VA 22030. Counsel shall arrange dates and times for access to review the source code. At no time shall the source code be removed from the iPad or the Carroll & Nuttall Law Office. Counsel for the defendant and any experts retained by the defense shall be allowed to take notes, but absolutely no videos, recordings or any other format of copying shall be made of the source code. Photographs will be allowed only upon the request of the defendant and written

authorization of Cybergenetics. If any parties deem it necessary, they may petition the Court for modifications of this Protective Order."

Response to defense reply

63. The defense "Reply to Government's Pretrial Motions" asks to "inspect the reliability of the statistical evidence." This is easily accomplished, at no cost to the defense, in accordance with established Daubert legal and forensic scientific standards, by simply testing the TrueAllele software on DNA data.

64. The "industry standard" in forensic science for the validation of systems has been established by widely accepted standards boards from the FBI, SWGDAM, ANSI, and NIST. The IEEE organization they mention does not establish forensic science standards.

65. The defense incorrectly claims that PG programs "cannot be objectively verified." First, with data modeling PG methods, the weight of evidence is a property of the DNA evidence, not the software. Second, such data modeling PG methods follow a predictable log-log relationship between contributor DNA amount and the DNA match statistic. Third, forensically accepted standards organizations have provided mechanisms for objective validation through testing. Fourth, the defense can test TrueAllele (at no cost) to scientifically assess their unfounded assertions. Fifth, Cybergenetics tested six different PG software programs (developed by different groups) on the lab's DNA data; all of the programs weighed the evidence and delivered the same result – there is statistical support for the presence of Lafon Ellis' DNA on the pistol.

66. The defense asserts that there has been no "independent review" of TrueAllele reliability. That assertion is incorrect. Validation studies have been conducted by scientists who do

not work for Cybergenetics. Almost all of Cybergenetics validation studies have coauthors (e.g., crime laboratories or academic scholars) who are independent of the company. The scientific journals, editors, and anonymous peer reviewers of the eight published validation papers were entirely independent. Moreover, the defense and their experts have the opportunity to test the TrueAllele software, conducting their own independent assessment.

67. The defense discusses the 2016 PCAST report. This policy report is not a scientific publication. The document contains no new testing or scientific evidence. The authors' opinions on PG methods flatly contradict the published peer-reviewed studies they cite. Moreover, NIST scientist Dr. John Butler is not an expert or innovator of PG methods, and had an inherent conflict of interest – his organization stood to gain fourteen million dollars from PCAST's federal funding recommendations (PCAST, page 129).

68. Scientific studies based on empirical testing entirely undermine PCAST's unfounded policy proposals for DNA mixture interpretation. For example, a recent peer-reviewed paper included the conclusions reproduced in the next paragraph. *See: Bauer DW, Butt N, Hornyak JM, Perlin MW. Validating TrueAllele® interpretation of DNA mixtures containing up to ten unknown contributors. J Forensic Sci. 2020;25(2):380-98.*

69. "The data showed that contributor DNA quantity determines mixture information and its variability. The 2016 President's Council of Advisors on Science and Technology (PCAST) policy report suggested limiting DNA mixture usage based on contributor number and mixture weight. Our empirical validation study underscores why this forensic policy proposal is scientifically unfounded:

1. The number of contributors, and their relative weight in a mixture, are merely factors affecting contributor DNA quantity—the main independent variable.
2. The linear relationship between DNA quantity and match information provides a useful predictive theory that explains match strength.
3. Mixture interpretation validation studies demonstrate a continuum of predictable match information (from none to all). There is no scientific evidence supporting PCAST's proposal to impose arbitrary limits."

70. The defense describes an admissibility outcome related to STRmix, a PG data modeling software program developed by New Zealand's Institute of Environmental Science and Research (ESR). Cybergenetics is not ESR. TrueAllele is not STRmix. While STRmix may use TrueAllele methods (as alleged in Cybergenetics' patent infringement suit against ESR), the ESR software was developed by a different company.

71. The defense describes a source code situation with FST, a PG drop out software program developed by New York City's Office of the Chief Medical Examiner (OCME). Unlike the private Cybergenetics company, OCME is a government agency that does not enjoy trade secret protection; TrueAllele is a trade secret, FST was not. Unlike TrueAllele, the FST source code was in the possession of the government; hence the prosecution was obligated to turn the documents over to the defense under *Brady v. Maryland*. Strikingly, OCME refused to let others, including outside scientists and defendants, have access to the FST executable program for testing, so no independent testing was possible; however, Cybergenetics makes its TrueAllele executable program available to defendants and others for independent testing.

Response to defense exhibits

72. Exhibit A, Canada Court Opinion. In R. v Dechamp, the Nova Scotia judge found TrueAllele to be reliable under all five prongs of Daubert. "[TrueAllele] can be well argued to pass the *Daubert* test for admission as that test has come to be interpreted and applied in the United States." (Paragraph 128)

    a. "TrueAllele has been subjected to testing and validation by a number of laboratories that have purchased the software for their use, and it has been extensively tested by Cybergenetics itself. The use of probabilistic genotyping for interpreting DNA mixtures has been tested." (Paragraph 133)
    b. "TrueAllele has been subjected to peer review and publication." (Paragraph 140)
    c. "The TrueAllele system has a known error rate. It provides an error rate for every case." (Paragraph 142)
    d. "There is nothing to suggest that Cybergenetics has failed to comply with any standards or laws that apply to it." (Paragraph 152)
    e. "Probabilistic genotyping has been accepted by many as a valuable enhancement to the ability to interpret complex DNA mixtures." (Paragraph 153)

73. Exhibit B, Adams Declaration. Forensic Bioinformatics employee Nathaniel Adams is not an expert in probabilistic genotyping. Having only a bachelor's degree level of computer science education, he has not developed PG software, validated PG software through normative scientific testing, published original scientific contributions about PG methods, determined PG error rates, or operated the TrueAllele software on evidence in criminal cases. As a defense expert, he has always declined the opportunity to actually test the

TrueAllele software on case or validation DNA data. He does not subscribe to Daubert or forensic standards regarding scientific testing and validation.

74. Exhibit C, Krane Declaration. Professor Dan Krane's questions about the TrueAllele model are addressed in peer-reviewed publications that describe the software's statistical model and computation; *see, for example: Perlin MW, Legler MM, Spencer CE, Smith JL, Allan WP, Belrose JL, et al. Validating TrueAllele® DNA mixture interpretation. J Forensic Sci. 2011;56(6):1430-47.* Additional modeling details that answer his questions are given in the disclosure document *TrueAllele Methods: Statistical Model*. Professor Krane can freely test the TrueAllele, applying the software method to DNA data, in order to assess the reliability of the program on case or validation data.

75. Exhibit D, Heimdahl and Matthews Declaration. The declarants range over many topics and software programs that are not relevant to TrueAllele or its reliability. Their recited figure of "six flaws for every thousand lines of code" from an introductory comment made in a paper published in 1999 may refer to outdated styles of error-prone noninteractive programming; it's hard to see its veracity or applicability here. In the disaster cases they describe, the problems were identified by testing the software on data (as done in normative science and Daubert), not by scrutinizing source code. They confusingly conflate "source code" (text) and "executable software" (application) by using the ill-defined phrase "executable source code." In paragraph 55, the declarants write, "Quite simply, other than by *running the program*, Mr. Ellis' expert cannot evaluate how the software actually operates, whether the results yielded by TrueAllele are reproducible, or whether it works the way that Cybergenetics claims." Exactly. The defense experts should run the

TrueAllele program to assess its reliability, rather than refuse to test the software as applicable standards require.

76. Exhibit E, SDNY Decision on OCME FST. As discussed above, the FST decision is not relevant to TrueAllele. There were no trade secrets in that case, the OCME government laboratory had disclosure obligations, and the lab did not allow independent or defense testing of their FST software program.

77. Exhibit F, SDNY Protective Order for OCME FST. There are trade secrets in this Lafon Ellis case, the federal government is not in possession of TrueAllele source code and cannot disclose what it does not possess, and Cybergenetics allows external and defense testing of TrueAllele. The SDNY case is entirely distinguished from this case, and the associated SDNY protective order which does not protect trade secrets is not applicable here.

78. Exhibit G, Stipulated Patent Protective Order. The protective order in Cybergenetics civil litigation is completely different from the unfettered access to source code that the defense seeks in this case. The stipulated "ATTORNEYS' EYES ONLY — SOURCE CODE" protective order protects trade secrets and sensitive information. Section 7(c) on protection of documents limits who may review the documents and for what purpose. Section 7(d) places additional restrictions on access to source code, including on-site inspection without production, standalone computer located at Cybergenetics counsel's office, visual monitoring of activities to ensure no unauthorized copying, advance notice, Cybergenetics-provided software viewing utilities, access logging, limited focused review, limited printing or paper copies, and no electronic access to source code. The access terms

are stricter than those found in the Fairfax, Virginia protective order of *Commonwealth v. Watson*.

79. Science and the law have normative standards for reliability, based on empirically testing software methods on forensic data. Cybergenetics provides such standard testing to defendants free of charge. The defense request ignores those accepted standards. And keeps studiously quiet about the key criterion – empirical testing.

I declare the above is true and correct under penalty of perjury under the law of the Commonwealth of Pennsylvania, executed this 17th day of January 2021 in Pittsburgh, Pennsylvania.

By: